



11/20/00

11-21-00  
Case Docket No. PHN 17,772

A

COMMISSIONER FOR PATENTS, Washington, D.C. 20231

Enclosed for filing is the patent application of Inventor(s):  
GEERT F.G. DEPOVERE ANTONIUS A.C.M. KALKER JAN EVELEENS

For: WATERMARK EMBEDDING AND DETECTION

**ENCLOSED ARE:**

- ☒ Associate Power of Attorney;  
☒ Information Disclosure Statement, Form PTO-1449 and copies of documents listed therein;  
☒ Preliminary Amendment;  
☒ Specification (10 Pages of Specification, Claims, & Abstract);  
☒ Declaration and Power of Attorney:  
 (2 Pages of a [ ] fully executed [X] unsigned Declaration);  
☒ Drawing (3 sheets of [ ] informal [X] formal sheets);  
☒ Certified copy of EUROPEAN application Serial No. 99203914.9;  
☒ Authorization Pursuant to 37 CFR 1.136(a)(3)  
☒ Other: RELATED CASES;  
☐ Assignment to

jc816 U.S. PTO  
09/716907  
11/20/00

## FEE COMPUTATION

CLAIMS AS FILED				
FOR	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE - \$710.00
Total Claims	11- 20 =	0	X \$18 =	0.00
Independent Claims	3 - 3 =	0	X \$78 =	0.00
Multiple Dependent Claims, if any			\$260 =	0.00
TOTAL FILING FEE . . . . .			=	\$710.00

**Please charge Deposit Account No. 14-1270 in the amount of the total filing fee indicated above, plus any deficiencies. The Commissioner is also hereby authorized to charge any other fees which may be required, except the issue fee, or credit any overpayment to Account No. 14-1270.**

[ ] Amend the specification by inserting before the first line the sentence: This is a continuation-in-part of application Serial No. , filed .

Edward W. Goodman, Reg. No. 28,613  
 Attorney  
 (914) 333-9611

## CERTIFICATE OF MAILING

☒ Express Mail Mailing Label No. **EL 458 218603**

Date of Deposit

**November 20, 2000**

I hereby certify that this paper and fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231

**Valerie T. Deas**  
 Name

**Valerie T. Deas**  
 Signature

Send correspondence and papers to Corporate Patent Counsel  
 U.S. Philips Corporation, 580 White Plains Road, Tarrytown, New York 10591

\\SERVER0\SYS2\WPDOCS\GO\APP.DOC

Variable	Mean	SD	Min	Max
Age	35.2	10.5	18	65
Gender	0.45	0.50	0	1
Marital status	0.65	0.48	0	1
Education	12.5	1.5	9	16
Income	15.2	5.8	5	35
Occupation	1.2	0.8	0	2
Health status	0.75	0.42	0	1
Stress level	2.8	1.2	1	5
Life satisfaction	3.5	1.0	1	5
Resilience	4.2	0.8	3	5
Optimism	3.8	0.9	2	5
Self-efficacy	4.0	0.7	3	5
Emotional stability	3.2	0.6	2	4
Empathy	3.0	0.5	2	4
Prosocial behavior	3.5	0.7	2	4
Aggression	2.5	0.4	1	3
Conformity	3.0	0.6	2	4
Autonomy	3.2	0.5	2	4
Openness	3.8	0.7	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	4
Conscientiousness	3.5	0.6	2	4
Neuroticism	2.8	0.5	1	3
Extraversion	3.0	0.6	2	4
Agreeableness	3.2	0.5	2	

Atty. Docket

PHN 17,772

GROUP ART UNIT:

EXAMINER:

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Prior to calculating the filing fee and examination, please amend the above-identified application as follows:

Page 1, before line 1, insert as a centered heading

line 1, delete in its entirety, and insert at the left margin --Field Of The Invention--;

line 6, delete in its entirety, and insert at the left margin --Description Of The Related Art--;

line 8, change "WO-A-99/45705." to --WO-A-99/45705,  
corresponding to U.S. Patent Application Serial  
No. 09/423,273, filed November 4, 1999.--;

line 26, after "(e.g." insert --,-- (comma);

Page 2, line 1, delete in its entirety, and insert as a centered  
heading --SUMMARY OF THE INVENTION--;

line 29, center the heading;

lines 30 and 32, change "schematically a" to  
--, schematically, a block--;

lines 31 and 33, change "invention." to --invention--;

Page 3, line 1, change "to illustrate" to --illustrating--;

line 2, change "detector." to --detector--;

line 3, after "show" insert --block diagrams of--;

line 4, change "invention." to --invention; and--;

line 5, after "shows" insert --a block diagram of--;

line 8, center the heading;

after "OF" insert --THE--;

lines 9 and 33, change "schematically a" to  
--, schematically, a block--;

line 20, change "selects" to --13 selects and applies--;

Page 4, line 8, after "otherwise" insert --,(comma);

line 11, after "in" insert --International Patent  
Application--;

change "It" to --The correlation circuit--;

line 20, change "being" to --having been--;

line 21, after "case" insert --,(comma);

Page 5, line 12, after "schematic" insert --block--;

lines 12 and 13, change "It" to --The embedder--;

lines 13 and 14, delete "which is";  
line 18, after "schematic" insert --block--;  
line 24, after "(e.g." insert --,-- (comma).

#### IN THE ABSTRACT

Page 10, before line 1, delete in its entirety, and insert as a

centered heading

--ABSTRACT OF THE DISCLOSURE--;

line 1, change "A" to --In a--;

line 2, change "signal is disclosed. The" to --signal,  
the--;

after line 8, delete in its entirety.

#### IN THE CLAIMS

Please amend the claims as follows:

1. (Amended) A method of embedding a watermark in an information signal, comprising the steps [of]:

[-] analyzing a given property of the information signal and determining an actual value of said property;

5 [-] associating different watermarks with distinct values of said property; and

[-] selecting the watermark associated with said actual value for embedding in the information signal.

2. (Amended) [A] The method as claimed in claim 1, in which the information signal is a sequence of video images, and said analyzing step [comprising] comprises:

5 analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

3. (Amended) [A] The method as claimed in claim 1, in which the information signal is a sequence of audio signal segments, and said analyzing step [comprising] comprises:

5 analyzing a shape of the frequency spectrum of said audio segments, each distinct shape of the frequency spectrum constituting a value of said property of the information signal.

4. (Amended) [A] The method as claimed in claim 1, in which  
the embedded watermark is a combination of two or more basic  
watermark patterns constituting a set of basic watermark patterns  
being selected from different sets in dependence upon the actual  
5 value of the property of the information signal.

5. (Amended) A method of detecting a watermark in an  
information signal, comprising the steps [of]:

[-] analyzing a given property of the information signal and  
determining an actual value of said property;

5 [-] associating different watermarks with distinct values of  
said property; and

[-] selecting and detecting the watermark associated with said  
actual value.

6. (Amended) [A] The method as claimed in claim 5, in which  
the information signal is a sequence of video images, and said  
analyzing step [comprising] comprises:

analyzing a spatial or temporal distribution of luminance  
5 values, each distinct distribution of luminance values constituting  
a value of said property of the information signal.

7. (Amended) The method as claimed in claim 5, in which the information signal is a sequence of audio signal segments, and the method [comprising] further comprises the [steps of] step:

calculating the frequency spectrum for each segment, each  
5 distinct shape of said frequency spectrum constituting a value of said property of the information signal.

8. (Amended) The method as claimed in claim 5, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of  
5 the property of the information signal.

9. (Amended) A watermark embedder for embedding a watermark in an information signal, comprising:

[-] means [(12)] for analyzing a given property [(P)] of the information signal and determining an actual value of said  
5 property;

[-] means [(14)] for associating different watermarks with distinct values of said property; and

[-] means [(13)] for selecting the watermark associated with said actual value for embedding [(11)] in the information signal.

10. (Amended) A watermark detector for detecting a watermark in an information signal, comprising:

[-] means [(22)] for analyzing a given property of the information signal and determining an actual value of said property;

[-] means [(24)] for associating different watermarks with distinct values of said property; and

[-] means for selecting [(23)] and detecting [(21)] the watermark associated with said actual value.

11. (Amended) [A] The watermark embedder as claimed in claim 9, wherein said watermark embedder further [including] comprises:

a watermark detector [as claimed in claim 10,] for detecting a watermark in an information signal, comprising:

means for analyzing a given property of the information signal and determining an actual value of said property;

means for associating different watermarks with distinct values of said property; and

means for selecting and detecting the watermark associated with said actual value; and [comprising]


means [(15)] for refraining from embedding the selected watermark in response to said watermark detector detecting said selected watermark in the information signal.



Figure 1 consists of 12 histograms arranged in a single column. Each histogram represents the distribution of the number of non-zero elements in the vector  $x$  for a specific value of  $n$ . The values of  $n$  are 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, and 120, listed from top to bottom. The x-axis for each histogram is labeled with the number of non-zero elements, and the y-axis is labeled with the frequency. As  $n$  increases, the distribution of non-zero elements shifts to the right, indicating that the vector  $x$  contains more non-zero elements as  $n$  grows.

The claims have been amended to more clearly define the invention as disclosed in the written description. In particular, claim 11 has been made a proper singularly dependent claim depending from claim 9. In addition, the claims have been amended for clarity.

Respectfully submitted,

by   
Edward W. Goodman, Reg. 28,613  
Attorney  
Tel.: 914-333-9611

Watermark embedding and detection.

## FIELD OF THE INVENTION

The invention relates to a method and arrangement for watermarking an information signal, for example, an audio or video signal. The invention also relates to a method and arrangement for detecting a watermark in such an information signal.

5

## BACKGROUND OF THE INVENTION

A known method of watermarking a video signal is disclosed in International Patent Application WO-A-99/45705. In this method, a watermark pattern is added to the video signal. A watermark detector correlates the same pattern with the suspect signal. If the correlation exceeds a given threshold, the pattern is said to be present. The presence or absence of the pattern represents a single bit of information. The embedded watermark may also carry a multi-bit payload. In the system disclosed in WO-A-99/45705, the payload is represented by a combination of one or more basic patterns and spatially shifted versions thereof. The payload is encoded into the respective shift vectors. The watermark detector correlates each basic pattern with the suspect signal, and determines the spatial positions of the basic patterns with respect to each other. The detector further checks whether said positions constitute a valid payload.

The process of correlating watermark patterns with the suspect signal requires the watermark detector to have locally stored versions of said patterns. In view thereof, it is desired that the watermarking system employs only a few different patterns. The patterns being used are kept secret to the outside world. However, even without knowledge of the patterns, a hacker can compromise the system if he has the relevant embedder at his disposal. He may feed an arbitrary input signal to said embedder and subtract the signal from its watermarked version. The difference signal thus obtained resembles the watermark of any other watermarked signal, depending on the perception model used in the watermark embedder at hand. If the difference signal is combined with (e.g. added to or subtracted from) a watermarked signal, the embedded watermark will substantially be cancelled or at least no longer represent a valid payload. In either case, the embedded watermark has been made ineffective.

## OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a more secure method and arrangement for embedding and detecting a watermark in an information signal, even if a hacker has a watermark embedder at his disposal.

5 To this end, the method in accordance with the invention comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with distinct values of said property, and embedding the watermark associated with said actual value. The corresponding watermark detection method comprises the steps of analyzing a given property of the information signal and determining an actual value of said property, associating different watermarks with  
10 distinct values of said property, and detecting the watermark associated with said actual value.

It is achieved with the invention that the embedded watermark pattern changes from time to time, as a function of the information signal content. Feeding an arbitrary signal to an embedder so as to produce a signal that resembles the watermark, as described above,  
15 does not work anymore because the arbitrary signal has different properties. A significant advantage of the invention is that the number of different watermark patterns which the detector must store can be kept much lower. Said number is a result of balancing detector complexity versus security.

There are numerous examples of properties of the information signal that can be  
20 used for selecting the watermark pattern to be embedded. The only requirement to be fulfilled is its robustness or invariance with respect to the embedded watermark. Advantageous examples of properties are distinct distributions of luminance values of a video signal, or distinct shapes of the frequency spectrum of an audio signal.

Further aspects of the invention are apparent from and will be elucidated with  
25 reference to the embodiments described hereinafter. The examples relate to watermark embedding and detection of video signals, but it will be appreciated that the invention equally applies to audio signals or any other type of multimedia signal.

## BRIEF DESCRIPTION OF THE DRAWINGS

30 Fig. 1 shows schematically a diagram of a watermark embedder in accordance with the invention.

Fig. 2 shows schematically a diagram of a watermark detector in accordance with the invention.

Fig. 3 shows an arrangement to illustrate the operation of the watermark embedder and detector.

Figs. 4 and 5 show further embodiments of the watermark embedder in accordance with the invention.

Fig. 6 shows a further embodiment of the watermark detector in accordance with the invention.

## DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 1 shows schematically a diagram of an embodiment of a watermark embedder **1** in accordance with the invention. It will here be assumed that the embedded watermark represents a 1-bit payload. For example, the absence of a watermark indicates that the video signal may freely be copied, whereas the presence of a predetermined watermark denotes that making a copy of the signal is prohibited.

The embedder receives an input video signal **I** in the form of a sequence of images, and comprises an adder **11** which adds a watermark pattern  $W_i$  to each image. The embedder further comprises an image analyzer **12**, a selector **13** and a read-only memory **14** in which a plurality of different watermark patterns  $W_1..W_N$  are stored. The analyzer **12** receives the video signal and analyzes a given property **P** of the video signal as a function of time. The actual value of property **P** found by analyzer **12** is applied to the selector **13**. In response thereto, the selector selects one of the stored watermark patterns  $W_1..W_N$  to the adder **11** for embedding.

The analyzer **12** may take numerous forms. A few examples will be given to provide sufficient teaching to enable a skilled person to design appropriate alternative embodiments. The property being analyzed may be the distribution of luminance values across the image (spatial distribution) or across a sequence of images (temporal distribution). In a first example, the analyzer divides each image into sub-images, and determines which of said sub-images has the highest average luminance. The relevant sub-image number is the actual value of property **P**. In a second example, the analyzer assigns a "0" to each sub-image having a low average luminance and a "1" to each sub-image having a high average luminance. Each video image is now characterized by an n-bit code, where n is the number of sub-images. The relevant n-bit code is the actual value of property **P**. The property being analyzed may also be local image activity. Such an analysis can easily be carried out in the frequency domain.

Fig. 2 shows schematically a diagram of a preferred embodiment of a watermark detector **2** in accordance with the invention. The detector receives a suspect video

signal J and comprises an image analyzer **22**, a selector **23** and a read-only memory **24** which are identical to the corresponding counterparts of embedder **1**. Accordingly, the analyzer **22** analyzes the same property P of the video signal, and the selector **23** selects the same watermark pattern W from the stored patterns  $W_1..W_N$ , as the embedder.

5           The detector further comprises a correlation circuit **21** which calculates the correlation between each image of the suspect video signal and the applied watermark pattern  $W_i$ . If the correlation exceeds a predetermined threshold, the selected watermark pattern  $W_i$  is said to be present ( $D=1$ ), otherwise it is said to be absent ( $D=0$ ).

10           The correlation circuit **21** is preferably of a type which performs the correlation for all possible spatial positions of the applied watermark with respect to the image. Such a correlation circuit is disclosed in WO-A-99/45705. It generates a correlation pattern which exhibits a peak for each spatial position of the watermark. WO-A-99/45705 describes that multiple peak positions may represent a payload. However, as mentioned above, the payload in this example is a 1-bit copy control signal. The detection circuit **2** will consider the presence  
15 of 2 or more peaks as an invalid payload ( $D=0$ ).

It is assumed that the watermark patterns  $W_1..W_N$  are secret and can neither be retrieved by interrogating the embedder or detector circuits. As will now be explained with reference to Fig. 3, the invention prevents a hacker from compromising the system when he happens to have an embedder at his disposal. In Fig. 3, a potential hacker receives a video  
20 signal V' being watermarked by an embedder **1a**. The signal V' may be a recorded signal, in which case the actual embedding took place a long time ago. The embedder **1a** is of a type as described above with reference to Fig. 1.

25           The hacker has an identical embedder **1b** at his disposal. An arbitrary video signal X is applied to said embedder **1b** so as to locally generate a watermarked video signal X'. An adder **3** subtracts the arbitrary signal X from its watermarked version X'. The difference signal (which strongly resembles the embedded watermark pattern) is then combined with (added to or subtracted from) the watermarked signal V' by a further adder **4**. The suspect signal V'' thus processed is applied to a watermark detector **2** as described above with reference to Fig. 2.

30           Without the provisions of the invention, both embedders **1a** and **1b** embed the same watermark in the respective input signals. This results either in a cancellation of the watermark in the suspect signal V'' or in an invalid payload due to multiple occurrences of the watermark pattern W at different positions. In both cases, the detector generates an output signal  $D=0$  and the hacking attack is successful.

With the provisions of the invention, the watermark  $W_i$  ( $i=1..N$ ) in signal  $V'$  will generally differ from the watermark  $W_j$  ( $j=1..N$ ) in signal  $X'$ , because the contents of the original video signals  $V$  and  $X$  are different. The property analysis algorithm of detector **2** responds to the contents of signal  $V''$  which is substantially equal to the contents of  $V$ .

- 5 Consequently, the watermark pattern being checked by detector **2** is the watermark pattern  $W_i$  which has been embedded by embedder **1a**. The detector ignores the additional presence of a different pattern  $W_j$ , and the hacking attack thus fails.

A possible work-around is feeding the watermarked signal  $V'$  instead of an arbitrary signal  $X$  to embedder **1b**, so as to force embedder **1b** to select the same watermark  $W_i$  as embedder **1a**. To avoid this, the embedders **1a** and **1b** are preferably of a type that refrains from embedding a watermark in a signal that has already been watermarked. Fig. 4 shows a schematic diagram of such an embedder. It comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as the embedder which is shown in Fig. 1. It further comprises the correlation circuit **21** of the detector which is shown in Fig. 2. The correlation circuit **21** detects whether the input signal  $I$  already includes the watermark pattern  $W_i$  to be embedded. If that is the case ( $D=1$ ), a switch **15** is controlled to prevent the watermark pattern  $W_i$  from being embedded multiple times.

Fig. 5 shows a schematic diagram of a watermark embedder for embedding multi-bit payload in the video signal. The embedder comprises the same adder **11**, image analyzer **12**, selector **13** and ROM **14** as described before with reference to Fig. 1. The ROM **14** now stores a plurality of sets of watermark patterns. The embedder further includes an encoding circuit **16** which receives a selected set  $i$  of basic watermark patterns  $W_{i,1}$ ,  $W_{i,2}$ , ..., and encodes a multi-bit payload  $d$  into the relative positions of said patterns. The basic patterns have a relatively small size (e.g.  $128 \times 128$  pixels). The watermark pattern generated by encoder **16** is subsequently tiled over the image by a tiling circuit **17**. The ROM **14** stores different sets of basic patterns for different values of signal property  $P$ . The actual set of basic patterns being applied to encoder **16** is controlled by the actual value of property  $P$  and changes as a function of time.

Fig. 6 shows the corresponding watermark detector. The detector comprises a folding circuit **25** for folding and storing image segments of  $128 \times 128$  pixels in a buffer prior to correlation. The detector further comprises the same correlation circuit **21**, image analyzer **22**, selector **23** and read only memory **24** as described before with reference to Fig. 2. The ROM **24** stores different sets of basic patterns for different values of signal property  $P$ . The

actual set of basic patterns being applied to the correlation circuit **21** is controlled by the actual value of property P.

It should be noted that the invention is not limited to the watermarking systems described in the embodiments. For example, a watermarking system is known that uses  $n$  different watermark patterns, each pattern corresponding to one bit of an  $n$ -bit payload. In accordance with this invention, the embedder and detector of such a system include different sets of  $n$  patterns. A particular set is then selected in response to the actual value of a signal property.

In summary, a method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark ( $W_i$ ) is selected (13) from a plurality of watermarks ( $W_1..W_N$ ) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. It is achieved with the invention that the embedded watermark changes from time to time as a function of the information signal content, so that it cannot easily be hacked.

## CLAIMS:

1. A method of embedding a watermark in an information signal, comprising the steps of:

- analyzing a given property of the information signal and determining an actual value of said property;

5 - associating different watermarks with distinct values of said property; and

- selecting the watermark associated with said actual value for embedding in the information signal.

10 2. A method as claimed in claim 1, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.

15 3. A method as claimed in claim 1, in which the information signal is a sequence of audio signal segments, said analyzing step comprising analyzing a shape of the frequency spectrum of said audio segments, each distinct shape of the frequency spectrum constituting a value of said property of the information signal.

20 4. A method as claimed in claim 1, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.

25 5. A method of detecting a watermark in an information signal, comprising the steps of:

- analyzing a given property of the information signal and determining an actual value of said property;

- associating different watermarks with distinct values of said property; and

- selecting and detecting the watermark associated with said actual value.

09716907 " 112000



6. A method as claimed in claim 5, in which the information signal is a sequence of video images, said analyzing step comprising analyzing a spatial or temporal distribution of luminance values, each distinct distribution of luminance values constituting a value of said property of the information signal.
7. method as claimed in claim 5, in which the information signal is a sequence of audio signal segments, the method comprising the steps of calculating the frequency spectrum for each segment, each distinct shape of said frequency spectrum constituting a value of said property of the information signal.
8. method as claimed in claim 5, in which the embedded watermark is a combination of two or more basic watermark patterns constituting a set of basic watermark patterns being selected from different sets in dependence upon the actual value of the property of the information signal.
9. watermark embedder for embedding a watermark in an information signal, comprising:
- means (12) for analyzing a given property (P) of the information signal and determining an actual value of said property;
  - means (14) for associating different watermarks with distinct values of said property; and
  - means (13) for selecting the watermark associated with said actual value for embedding (11) in the information signal.
10. A watermark detector for detecting a watermark in an information signal, comprising:
- means (22) for analyzing a given property of the information signal and determining an actual value of said property;
  - means (24) for associating different watermarks with distinct values of said property; and
  - means for selecting (23) and detecting (21) the watermark associated with said actual value.
11. A watermark embedder as claimed in claim 9, further including a watermark detector as claimed in claim 10, and comprising means (15) for refraining from embedding the



**ABSTRACT:**

A method and arrangement for embedding and detecting a watermark in an information signal is disclosed. The embedded watermark ( $W_i$ ) is selected (13) from a plurality of watermarks ( $W_1..W_N$ ) in dependence upon a property P of the signal. An example of such a property is the distribution of luminance values of the current video image as calculated by an analysis circuit (12). The corresponding watermark detector performs the same operation: the watermark being looked for depends on the same signal property. It is achieved with the invention that the embedded watermark changes from time to time as a function of the information signal content, so that it cannot easily be hacked.

10      Fig. 1

1/3

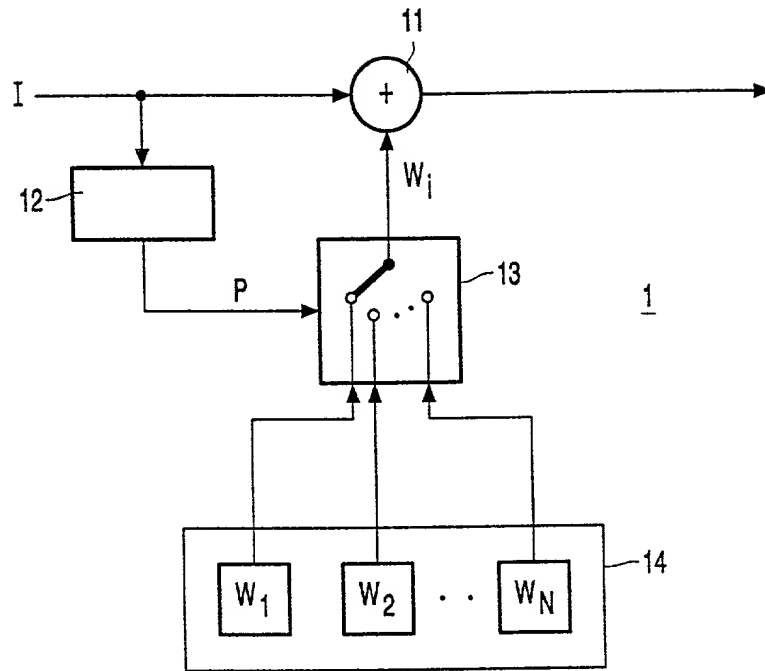


FIG. 1

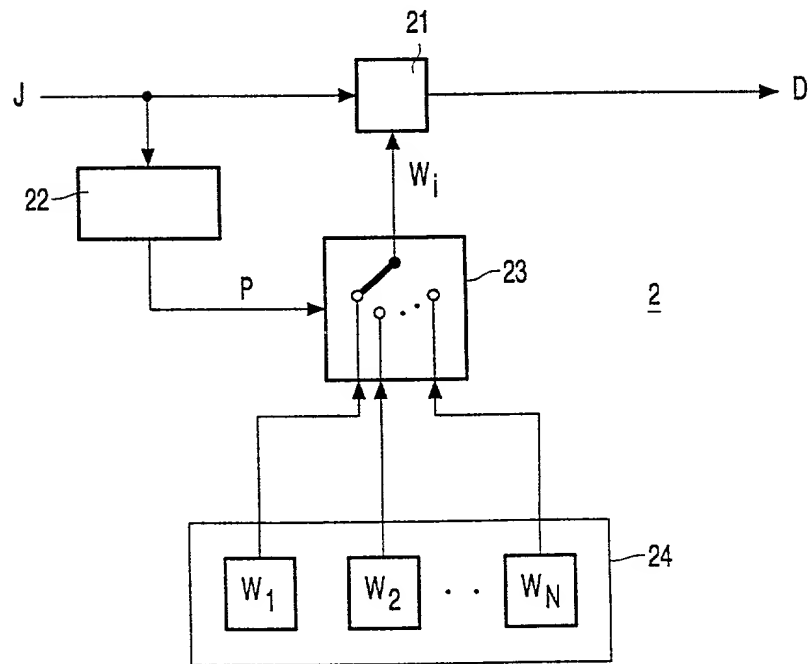


FIG. 2

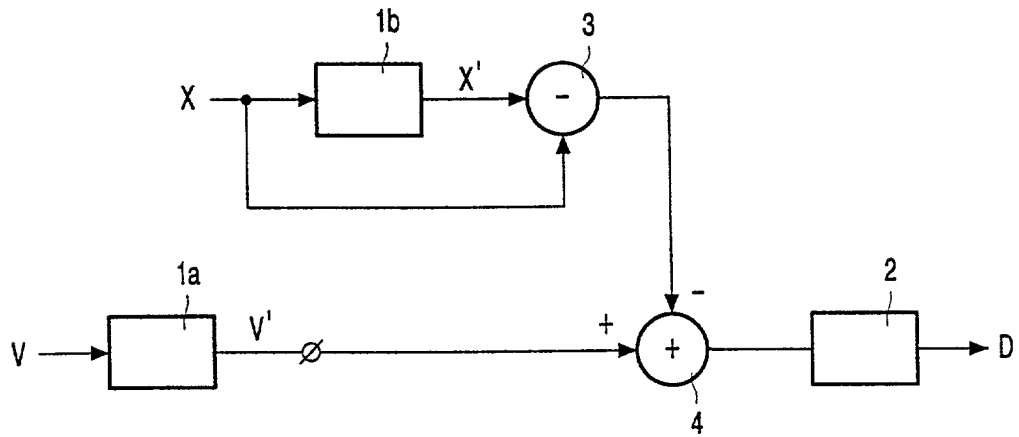


FIG. 3

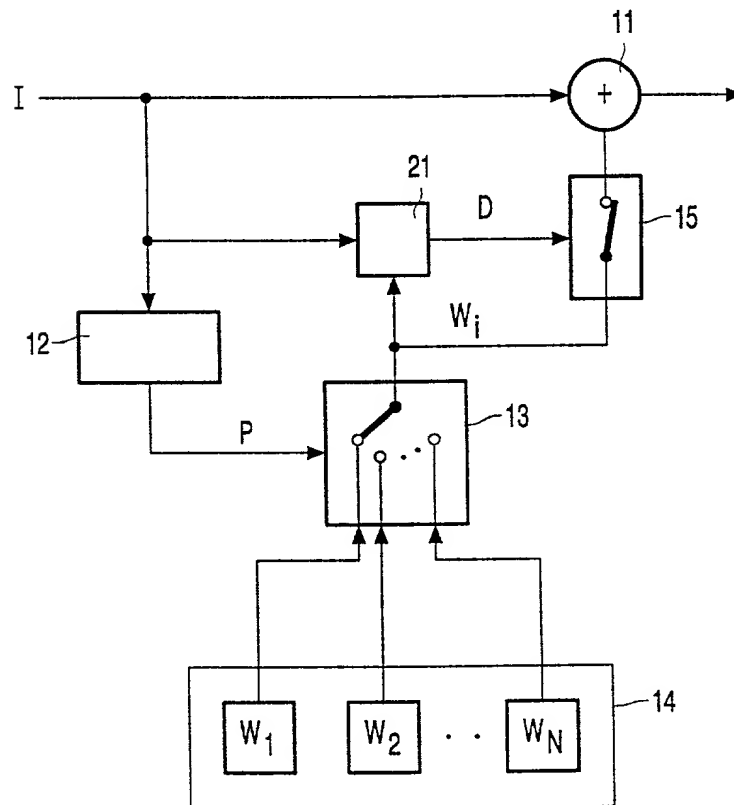


FIG. 4

3/3

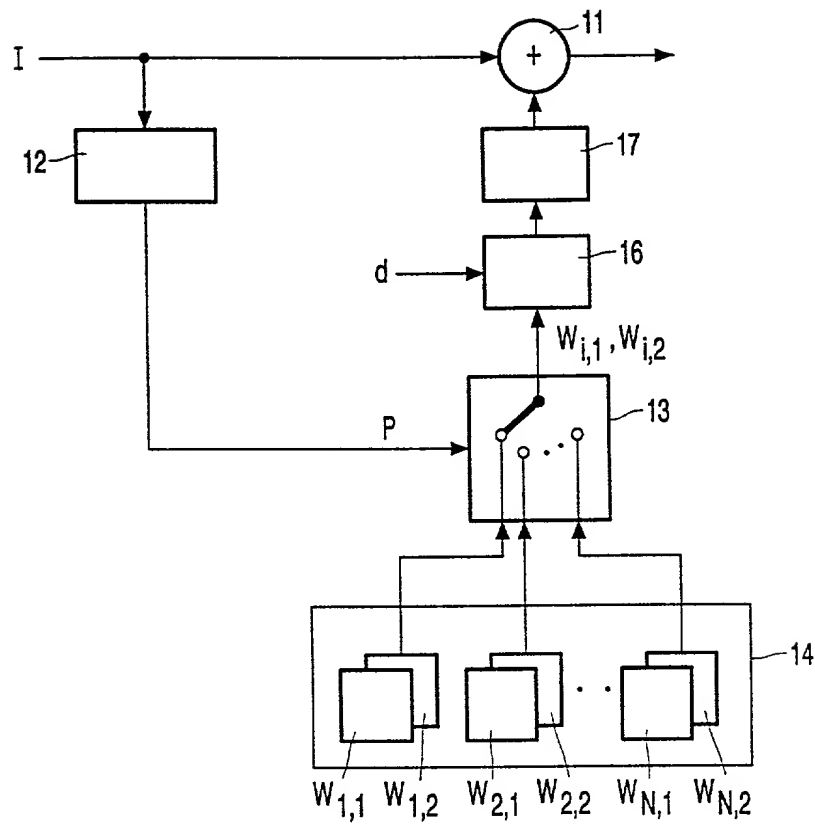


FIG. 5

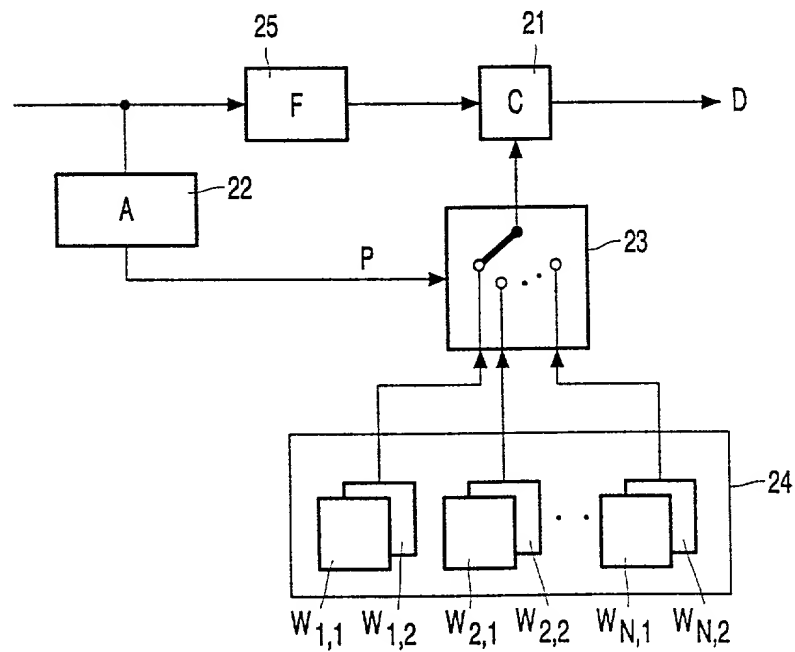


FIG. 6

# DECLARATION and POWER OF ATTORNEY

ATTORNEY'S DOCKET NO.:  
**PHN 17.772 US**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled  
**"Watermark embedding and detection"**

the specification of which (check one)

☐ is attached hereto.

☐ was filed on \_\_\_\_\_ as Application Serial No. \_\_\_\_\_ and was amended on \_\_\_\_\_ (if

applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

## PRIOR FOREIGN APPLICATION(S)

COUNTRY	APP. NUMBER	DATE OF FILING (DATE, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119
Europe	99203914.9	23 November 1999	YES

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

## PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Jack E. Haken, Reg. No. 26,902

Michael E. Marion, Reg. No. 32,266

Edward M. Blocker, Reg. No. 30,245

SEND CORRESPONDENCE TO: Corporate Patent Counsel;  
U.S. Philips Corporation; 580 white Plains Road;  
Tarrytown, NY 10591

DIRECT TELEPHONE CALLS TO:  
(name and telephone No.)  
(914) 332-0222

Dated:		Inventor's Signature:	
Full Name of in Inventor	Last Name <b>DEPOVERE</b>	First Name <b>Geert</b>	Middle Name <b>Florimond Gerard</b>
Residence & Citizenship	City <b>Eindhoven</b>	State of Foreign Country <b>The Netherlands</b>	Country of Citizenship <b>Belgium</b>
Post Office Address	Street <b>Prof. Holstlaan 6</b>	City <b>5656 AA Eindhoven</b>	State of Country <b>The Netherlands</b>
Dated:		Inventor's Signature:	
Full Name of in Inventor	Last Name <b>KALKER</b>	First Name <b>Antonius</b>	Middle Name <b>Adrianus Cornelis Maria</b>
Residence & Citizenship	City <b>Eindhoven</b>	State of Foreign Country <b>The Netherlands</b>	Country of Citizenship <b>The Netherlands</b>
Post Office Address	Street <b>Prof. Holstlaan 6</b>	City <b>5656 AA Eindhoven</b>	State of Country <b>The Netherlands</b>

Dated:		Inventor's Signature:		
Full Name of in Inventor	Last Name <b>EVELEENS</b>	First Name <b>Jan</b>	Middle Name	
Residence & Citizenship	City <b>Eindhoven</b>	State of Foreign Country <b>The Netherlands</b>	Country of Citizenship <b>The Netherlands</b>	
Post Office Address	Street <b>Prof. Holstlaan 6</b>	City <b>5656 AA Eindhoven</b>	State of Country <b>The Netherlands</b>	Zip Code
Dated:		Inventor's Signature:		
Full Name of in Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State of Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State of Country	Zip Code
Dated:		Inventor's Signature:		
Full Name of in Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State of Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State of Country	Zip Code
Dated:		Inventor's Signature:		
Full Name of in Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State of Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State of Country	Zip Code
Dated:		Inventor's Signature:		
Full Name of in Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State of Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State of Country	Zip Code



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of  
GEERT F.G. DEPOVERE ET AL.

Atty. Docket

PHN 17,772

Filed: CONCURRENTLY

WATERMARK EMBEDDING AND DETECTION

Commissioner for Patents, Washington, D.C. 20231

APPOINTMENT OF ASSOCIATES

Sir:

The undersigned Attorney of Record hereby revokes all prior appointments (if any) of Associate Attorney(s) or Agent(s) in the above-captioned case and appoints:

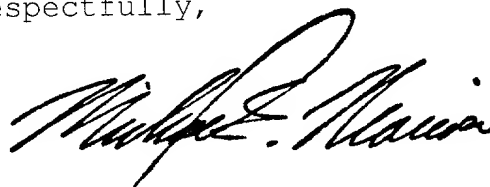
**EDWARD W. GOODMAN**

**(Registration No. 28,613)**

c/o U.S. PHILIPS CORPORATION, Intellectual Property Department, 580 White Plains Road, Tarrytown, New York 10591, his Associate Attorney(s)/Agent(s) with all the usual powers to prosecute the above-identified application and any division or continuation thereof, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED ATTORNEY OF RECORD.

Respectfully,



Michael E. Marion, Reg. 32,266  
Attorney of Record

Dated at Tarrytown, New York  
on November 6, 2000.